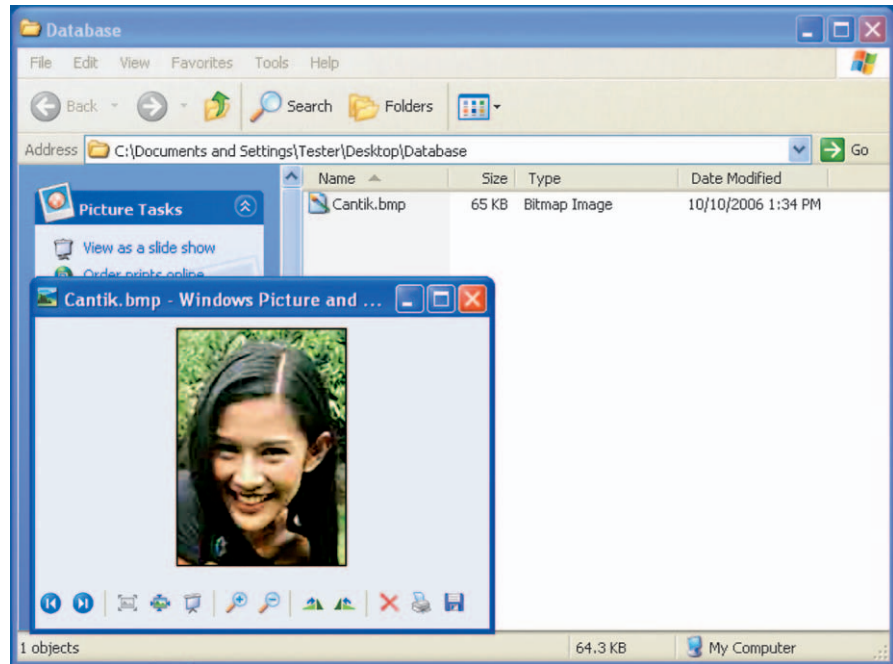
Virus Pemusnah Massal

Bagaikan senjata pemusnah massal yang sangat menakutkan itu, virus ini juga ternyata memiliki peran yang tidak jauh berbeda. Bagaimana tidak ngeri, coba Anda bayangkan apabila data atau dokumen yang dikerjakan sehari, sebulan, atau bahkan bertahun-tahun hilang begitu saja.

Arief Prabowo

Kita pasti kesal apabila itu terjadi. Dan dapat Anda bayangkan, itu mungkin baru satu komputer, tapi bagaimana bila misalnya itu terjadi pada satu kantor atau mungkin satu kota? *Gak kebayang kan* berapa total kerugiannya. Tapi, memang itulah sedikit gambaran yang terjadi, yang pada beberapa waktu yang lalu sempat membuat heboh.

Virus penghancur data ini dikenal oleh PCMAV sebagai virus Aduhai. Dan PCMAV sudah mengenali dua jenis varian dari virus ini, yakni Aduhai.A dan Aduhai.B. Ia dibuat menggunakan bahas Visual Basic yang di-*compile* dengan metode P-Code. Virus yang ber-icon-kan mirip folder standar Windows ini juga di-*compress* menggunakan UPX. Sehingga ukuran file/tubuhnya menjadi

PCMAV dapat mengatasi virus Aduhai.

Menciptakan file bergambar Dian Sastro.

sebesar 43.008 bytes untuk Aduhai.A dan 42.496 bytes untuk Aduhai.B.

Pada sistem yang kami uji coba, virus ini berjalan mulus pada Windows 98 SE dan Windows XP. Antivirus lain ada yang mengenal virus ini dengan nama Pacar, DelCanti, atau VB.AN. Bahkan ada beberapa antivirus luar menyebutkan bahwa virus ini masih merupakan varian dari virus Brontok/Rontokbro.Kenapa bisa *gitu ya*? Padahal ia bukanlah varian dari Brontok, karena ini adalah virus yang berbeda.

Infeksi File dan Memory

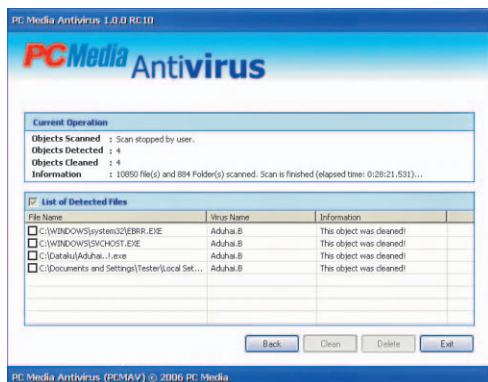
Pada saat kali pertama virus dijalankan, ia akan membuat beberapa file induk yang ia tanamkan pada sistem tersebut, di antaranya pada \%WINDOWS%\SVCHOST.EXE, \%WINDOWS%\system\SVCHOST.EXE, \%SYSTEM32%\EBRR.EXE, dan \%SYSTEM32%\mmtask.exe. Lalu ia memanggil keempat file induk tersebut agar aktif di memory. Jadi pada memory paling tidak terdapat empat buah *process* dari virus tersebut dengan nama process sama seperti nama file induknya.

Apabila virus ini berjalan pada *operating system* Windows 98, process dari virus ini tidak akan terlihat pada Task Manager karena ia sembunyikan dengan cara meregister process-nya sebagai *service* dengan menggunakan perintah API RegisterServiceProcess.

Virus Aduhai ini juga akan saling menjaga keharmonisan hubungan antartemannya di memory. Contohnya apabila dari keempat process virus tersebut ada yang hilang dari memory, entah itu sengaja di-*kill* oleh user atau karena sebab lain, maka dengan segera virus akan memanggil kembali process yang hilang itu. Ini merupakan salah satu cara sang virus agar susah dibunuh.

Ia juga akan memonitor setiap aplikasi yang dijalankan dan mencari setiap *window* dengan *class* berupa "CabinetWClass", yang mana class ini merupakan bagian dari class Windows Explorer untuk mencari tau drive/direktori yang sedang diakses oleh user. Apabila drive tersebut berupa Removeable Disk seperti contohnya Disket atau FlashDisk, ia akan segera membuat duplikat file virus ke drive tersebut. Tentunya menggunakan nama-nama file yang menarik, agar user tertarik mengkliknya.

Beberapa nama file tersebut, di antaranya "Agnes Monica.exe", "Foto Pacar.exe", "Bekas Pacar.exe", "Dian Sastro.exe", dan lain sebagainya. Lalu, setelah file tersebut berhasil diciptakan, ia akan langsung meng-

eksekusinya. Alhasil, file tersebut tidak bisa dihapus karena masih aktif di memory.

Infeksi Registry

Seperti halnya virus lain, Aduhai juga akan menginfeksi registry. Pada sistem Windows XP, ia akan menginfeksi registry yang terletak pada HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell dan HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell dengan cara mengalihkan nilai dari Shell tersebut yang seharusnya mengarah kepada file 'explorer.exe' dialihkan agar mengarah kepada file induk virus tersebut.

Sementara itu pada Windows 98, ia akan menginfeksi key HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\ dengan menambahkan item dengan nama "By: 05062705056127019455" dan pada key HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce\ dengan menambahkan item "Made In Ambon Manise—Sebagai PeSaN Anti korupsi".

Nilai dari kedua item tersebut juga diarahkan kepada file induk virus. Dengan menginfeksi run section pada key-key registry tersebut, nantinya saat memulai Windows virus ini akan aktif otomatis.

Apabila Anda lihat pada Windows Explorer, pasti setiap file aplikasi/executable *type information*-nya berupa "File Folder" bukan seperti yang biasanya, yakni "Applications". Itu bisa terjadi karena virus tersebut mengubah nilai registry pada HKLM\SOFTWARE\CLASSES\exefile\, yang tadinya berupa "Applications" menjadi "File Folder".

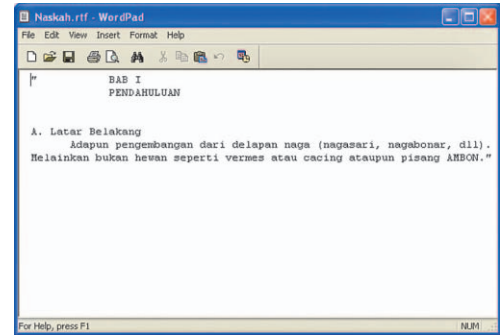
Dan walaupun pada virus ini Folder Options tidak disembunyikan seperti halnya yang dilakukan oleh virus-virus lain, tapi tetap saja ia mengisenginya dengan memanipulasi nilai *default* dari beberapa item pada registry untuk Folder Options tersebut. Yakni, pada HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\HideFileExt\UncheckedValue dan HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden\UncheckedValue.

Jadi, walaupun Anda melakukan perubahan pada Folder Options untuk menampilkan extensions pada setiap file dan menampilkan file system, tapi tetap saja tidak akan berpengaruh, karena *setting*-annya akan kembali seperti yang telah ia set.

Saatnya Beraksi

Virus yang dapat menyebar melalui media penyimpan data atau removeable disk seperti disket atau flash disk ini juga dapat menyebar melalui jaringan melalui *sharing directory*. Yakni, apabila direktori yang di-*share* mengandung virus dan virus tersebut diakses oleh komputer lain di jaringan tersebut, maka komputer yang mengaksesnya juga akan terinfeksi.

Pada saat file virus dieksekusi, ia juga terkadang akan membuat sebuah direktori di bawahnya dengan nama sama seperti nama file virus yang dijalankan dan diberi *attribut system* dan *hidden* agar tidak terlihat. Pada saat file virus tersebut diklik ia akan menampilkan isi dari direktori yang telah ia buat sebelumnya itu. Isinya adalah file "Naskah.rtf" atau "Cantik.bmp".

Dari tubuh sang virus setelah dilakukan proses *disassemble*, terlihat bahwa ia diprogram menggunakan sebuah form yang berisi tiga buah timer dan satu buah komponen *image* tempat menampung gambar Dian Sastro yang nantinya akan di-*extract* menjadi file "Cantik.bmp" tadi. Timer tersebut memiliki peranan masing-masing. Dan ada salah satunya dengan nama KillBill yang bertugas untuk memonitor setiap perubahan waktu yang terjadi.

Pesan dari pembuat virus.

Seperti yang dikatakan di awal, virus ini merupakan virus "pemusnah massal" yang dapat menghapus semua data Anda tanpa ampun. Itu dapat terjadi apabila pada komputer Anda bulan menunjukkan pada angka 10 (Oktober) dan tanggal ganjil. Serta apabila bulan menunjukkan pada angka 12 (Desember) dan tanggal berapapun. Jika salah satu kondisi tersebut terpenuhi, maka ia akan menjalankan fungsi DelAllFile seperti yang terlihat pada rutin di tubuh virus tersebut.

Virus ini akan menghapus semua file, tanpa terkecuali file systen dari Windows-nya sendiri, dan itu pula yang menyebabkan komputer tidak bisa *booting* dengan menampilkan pesan berupa "NTLDR is missing". Apabila itu terjadi hanya pada satu komputer, mungkin belum tentu diakibatkan oleh virus. Tapi, bagaimana misalnya bila itu terjadi pada sebuah kantor secara serentak?

Pembasmian dan Pencegahan

Untuk mengembalikan data yang hilang akibat dihapus oleh virus ini, coba dengan menggunakan *software data recovery*, mungkin masih bisa diselamatkan. Dan ingat, bulan Oktober dan Desember Aduhai akan menghapus data Anda, jadi hati-hati dan selalu *scan* komputer Anda dengan antivirus *update* terbaru. PC Media Antivirus sudah dapat mengatasi virus ini dengan baik hingga tuntas dan akurat 100%.

Untuk melakukannya, silakan Anda scan seluruh drive dengan PCMAV. Namun, apabila ternyata PCMAV tidak juga dapat mengenali virus Aduhai yang jelas–jelas telah menginfeksi komputer Anda, dengan senang hati kami akan menerima contoh virus yang Anda kirimkan. Kami tunggu! ■

Virus yang mirip dengan folder dan *type information* pada file *executable* yang berubah menjadi "File Folder".